

RECEIVED

JAN 14 1994

FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C.

DOCKET FILE COPY ORIGINAL

In the Matter of
Policies and Rules
Concerning Toll Fraud

)
)
)
)

CC Docket No. 93-292

COMMENTS

OF

THE SOUTHERN NEW ENGLAND TELECOMMUNICATIONS CORPORATION

The Southern New England Telecommunications Corporation (SNET), pursuant to Section 1.773 of the rules of the Federal Communications Commission (Commission) and the Commission's Notice of Proposed Rulemaking (NPRM),¹ hereby files its Comments in this proceeding.

I. Introduction

Toll fraud is an increasing industry problem which does not recognize geographic boundaries among states or telecommunications companies. Nor does it limit itself to a

¹ Policies and Rules Concerning Toll Fraud, Notice of Proposed Rulemaking, CC Docket No. 93-292, FCC 93-496, released December 2, 1993.

No. of Copies rec'd
List ABCDE

244

particular carrier. Fraud may occur over the facilities of an Interexchange Carrier (IXC), an Information Provider (IP), an Operator Service Provider (OSP), a Local Exchange Carrier (LEC) or a Cellular Carrier. Just as toll fraud has been identified as a universal industry problem, the solution should also be a strong, combined and concerted effort to combat the millions of dollars lost each year.

II. Increased Anti-Toll Fraud
Efforts Are Needed Now.

Additional coordination among the various institutions fighting toll fraud is essential. SNET believes that the Commission can and should play an active role in fostering that coordination. Similar to its efforts regarding the Network Reliability Council, the Commission should establish a Federal Advisory Committee (FAC) on Toll Fraud. The Committee should be established for a limited duration and for the specific purpose of developing and recommending specific action items necessary to fight toll fraud. Its charter should be broadly defined to allow the Committee to deal with the technical, regulatory and legislative issues involved. Representation on the Committee should include communications customers, service providers, manufacturers, law enforcement agencies and regulators.

III. Laws Should be Strengthened to Give
Law Enforcement Agencies Power to Act.

SNET supports federal legislation that clearly addresses the technological complexities associated with toll fraud crimes. In conjunction with federal legislation, stronger penalties are needed to assist law enforcement agencies in the prosecution of these crimes². Generally, law enforcement agencies have limited resources to dedicate to high technology toll fraud investigations, and in many cases where arrests are made, courts sentence offenders to probation and restitution. Because of high case loads in state probation offices, limited or no followup with convicted perpetrators of toll fraud occurs.

SNET recognizes the difficulties facing law enforcement agencies in attempting to prosecute toll fraud offenders. Not only do law enforcement agencies typically rely on state statutes as the basis for fraud prosecution, they also have limited technical abilities and resources to pursue the perpetrators. At the request of various law enforcement agencies, SNET provides training in recognizing and investigating toll fraud and other criminal activities associated with telecommunications within Connecticut. This training is designed to encourage police departments to dedicate personnel to the

² Testimony of Robert H. Rasor, Special Agent in Charge, Financial Crimes Division, U.S. Secret Service, Department of the Treasury, before the FCC en banc Hearing on Toll Fraud, October 9, 1992:

"A balance must quickly be struck between prosecutive, preventive measures and the ability of law enforcement to clearly show that individuals who deal in these types of crimes will be arrested, prosecuted and put in jail. Until such time as it becomes unprofitable and dangerous for the criminal element to play on this field, they will."

investigation of telephone-related fraud and other high technology investigative activity.

In addition to locally available training, SNET encourages law enforcement participation in professional organizations such as the International Association of Credit Card Investigators and the High Technology Crime Investigation Association. These organizations' objective is to bring together law enforcement and high technology industry representatives to share information. Specific training in high technology investigations, such as that provided by some federal agencies,³ can greatly enhance law enforcement's capability for successful and timely toll fraud investigations.

Today, however, these efforts, while valuable, tend to be local or ad hoc, and certainly lack the sort of comprehensiveness that this effort deserves. Federal legislation should encourage the development of the technical resources necessary to prevent and to prosecute toll fraud. The FAC could serve a major role in recommending legislation that would provide law enforcement agencies with tools for fraud prevention.

IV. SNET Supports the Work Being Done By the Toll Fraud Prevention Committee.

SNET supports the work being done by the Toll Fraud Prevention Committee (TFPC), a national, industry-wide forum made up of approximately 90 companies, including RBOCs, GTE, USTA, AT&T, MCI, Sprint, Allnet, Bell Canada, Stentor, Bellcore, Telus,

³ Such as the U.S. Secret Service, Federal Bureau of Investigation.

and a number of other Interexchange Carriers, as well as local exchange carriers (including SNET). The TFPC is associated with the Network Operators Forum (NOF), which is sponsored by the Alliance for Telecommunications Industry Solutions (formerly the Exchange Carrier Standards Association).

NOF provides a work forum for all telecommunications' industry participants to identify industry-wide operations issues involving the installation, testing and maintenance of exchange access and telecommunications network interconnection. In addition, NOF identifies issues related to network integrity and reliability. Resolutions to issues are developed by consensus agreement for voluntary implementation by the industry.

The TFPC provides the opportunity for all companies involved in telecommunications to come together as a group for the sharing of information and concerns about the multitude of fraudulent schemes perpetrated against the industry.

SNET's concerns regarding the increasing level of fraud led SNET to develop its Fraud Control System (FCS), which was introduced in January, 1993. FCS provides a sophisticated fraud detection and protection system that is designed to protect operator service providers, aggregators, payphone providers, interexchange carriers and local exchange carriers' networks from fraudulent use of line-based calling cards and commercial credit cards. Using proprietary screening parameters, the system provides customers with a real-time monitoring capability that is currently controlled by the Line Identification Database (LIDB).

FCS works in conjunction with the LIDB Gateway that provides access to all LIDBs in the United States and Canada. It includes services such as original line number screening, calling card validation, billing number screening, calling card fraud and public telephone checks.

SNET supports a strong facilitator role for the Commission in fighting toll fraud and the Commission's suggestion for a FAC on toll fraud. In particular, the effort of the TFPC/NOF should be encouraged by the FCC.

V. LECs' LIDB Validation Systems Provide the First Line of Defense to Limiting Fraud.

The LECs' LIDB system was created to provide an account status validation service for joint use calling cards and to determine any line restrictions for bill-to-third and collect calls. These services provide IXCs, LECs and other customers with a first line of defense against fraudulent usage as these systems provide the most up-to-date information available.

In order for these systems to be effective, however, all carriers must take full advantage of them to curtail fraudulent usage, and in some cases, stop it completely. Carriers that do not utilize the LIDB services must be prepared to accept the consequences of fraudulent use. The LECs must not be expected to share in the liability for fraud if carriers fail to access and utilize these validation services. Unless there is full and complete cooperation from all carriers to ensure that

call validation has been done before call processing, LEC liability for fraud should not be memorialized in tariffs.

A. LECs Must Be Provided With the Calling and Called Number.

The carriers querying the LIDB system should be required to provide the calling party number and the called numbers. This information is essential to permit LECs to identify areas where fraudulent activity originates and terminates. The Commission has already recognized the value of sharing this data in the LIDB Order:

We note that while each LIDB provider should maintain an accurate, up-to-date database, it is essential that LIDB customers also assist in this process. Reciprocity in the sharing of data is helpful to ensure that database information concerning the status of the line or calling card is the most current. Since fraud can only be battled effectively through cooperation among the users of the network, it is important that LIDB customers do their part.⁴

Many LECs have recently deployed anti-fraud systems that enhance their fraud detection capabilities. Without the provision of all information contained in the query (such as the calling party and the called numbers), LECs may not be able to identify, monitor and deter fraudulent activity.

The presence or absence of originating calling party number and the called numbers should affect the allocation of

⁴ See Local Exchange Carrier Line Information Database Order, CC Docket No. 92-24, released August 23, 1993, 8 FCC Rcd 7135, ¶33.

liability for toll losses. IXC's are in the unique position of having the information necessary to reduce toll fraud. The failure of an IXC to provide the calling party number should be a factor in assigning liability for any resulting fraud. LEC fraud detection capabilities can be considerably enhanced with the provision of calling party number by allowing for earlier detection and notification of fraudulent calling. By withholding the calling party number, IXC's restrict LEC's' ability to prevent fraud, thus creating costs and inefficiencies that are clearly not in the public interest.

B. IXC's Should Not Be Permitted to Charge for Calling Party Number.

Because the goal of the LEC's and IXC's in sharing this information is to reduce fraud, carriers should not be permitted to charge for the provision of anti-fraud information. IXC's currently have the calling party number as part of the call information necessary to route and bill toll calls. This information could easily, and at minimal cost, be included as part of the query forwarded to the LIDB database. The benefit in reduced toll fraud for the IXC's and their customers far outweighs any costs that the IXC's might incur to provide this information.

VI. Cellular/Wireless Telecommunications
Fraud Issues.

A. Liability for the Cost of Fraud
Rests With the Party Controlling
the Exposure.

SNET believes that the liability for the fraud connected with the use of a wireless (e.g. cellular) access device must be determined based on who initially controls the event that generated the specific fraudulent activity, rather than on who receives the service revenue.

Cellular fraud occurs as a result of a weak or exposed point in the interactive circle involving the provisioning, the use and the delivery of wireless service. These exposures result in such fraudulent activities as: 1) The production and use of an illegally or unauthorized, modified piece of access equipment (counterfeit or clone); 2) An erroneous or unauthorized entry to a database (e.g., Cellular Switch Positive File, Cellular Industry Negative File, Line Information Database); and 3) The use of the Mobile Identification Number (MIN) as a credit device (i.e., calling card) without the authorization of the cellular carrier.

Access to the hardware, software, information and equipment that allows these fraudulent activities to occur is alternately controlled by the carriers (cellular, LEC, IXC), manufacturers (mobile unit, switch, call site), distributors (resellers, dealers, agents), vendors (billing, clearing database, fraud prevention), and the end-users, or customers, themselves.

Although SNET believes that most liability questions are best handled through normal, open business negotiations or contracts, the various areas of exposure and responsibility should receive formal recognition. Carriers, manufacturers, distributors and vendors all have the responsibility to: 1) protect from any unauthorized or illegal access, extraction or modification, the data they maintain, the products they manufacture or distribute, and the services they provide; 2) ensure their products and services are error free and delivered at expected performance levels; 3) ensure their customers are educated as to what constitutes cellular fraud, what steps each should take to control exposures and, therefore, where each party's responsibilities or liabilities lie; and 4) immediately report (to the affected party), and rectify, any incidents of failure in their efforts to fulfill their responsibilities.

In addition, carriers are responsible for performing appropriate database inquiries, validations and authentications as required to determine if a particular service or feature may be rendered. This includes basic service, calling capabilities and restrictions, and credit and collect calls. End-users have the responsibility to: 1) protect the accessibility to the mobile unit as well as any documentation which contains their ESN/MIN combination; 2) conform to reasonable precautionary methods and features (PINs, A-KEY, call restrictions) as made available by the carrier; 3) immediately report such items as stolen units, unrecognized calls on bills, unauthorized use of the unit, and service problems which could lead to or be the

result of fraudulent calls); and 4) not utilize unauthorized or illegally modified access equipment.

B. Stronger Legislation is Required.

SNET supports the position that legislation is needed to empower the Justice Department to enforce FCC equipment rules, and to clarify cellular's position under Title 18, U.S.C. Section 1029, which makes it a federal crime for anyone to use, manufacture or traffic in counterfeit or unauthorized access devices and protect the use of tools which modify wireless telecommunications devices.

The anti-tampering rules of the FCC, as spelled out in Revision of Part 22 of the Commission's Rules Governing the Public Mobile Service (Notice of Proposed Rulemaking), 7 FCC Rcd 3658, 3741 (1992), need to become more than rules. They must become law, and be extended to apply not only to the equipment but also to the subsequent production and use of an unauthorized, modified piece of access equipment (counterfeit or clone). Such actions must be illegal, with appropriate penalties enforceable in a criminal court of law.

Although tumbling fraud is on the decline, it and its successor - counterfeiting - need to be clearly defined and positioned within U.S.C. Section 1029 or subsequent legislation. The wireless industry is at a distinct disadvantage in the area of fraud prosecution as a result of the current law's failure to define clearly its applicability to wireless communications. Specifically, new legislation needs to include: 1) the production, modification, possession or use of an unauthorized or

modified piece of access equipment; 2) the production, modification, possession or use of a computer, software, device, piece of equipment or tool which can produce or modify an unauthorized piece of wireless access equipment; and 3) an unauthorized access, addition, deletion or modification to a service- or feature-determining database (e.g., Cellular Switch Positive File, Cellular Industry Negative File, Line Information Database). Only with such specific legislation, will law enforcement agencies have the authority to begin to address the cellular fraud problem.

C. Need to Share Information.

SNET feels that all participants (carriers, manufacturers, distributors, vendors and law enforcement agencies) be legally permitted to share detailed information when there is suspected fraud. A clear set of rules, based on law, which clearly define the specifics regarding the exchange of information, need to be developed and adopted. In order to accomplish this, the rules must clearly define: 1) the circumstances under which information is to be shared; 2) the detail and content of the exchanged information; and 3) a vehicle or process which protects all of the parties involved.

D. Carriers Have the Right to Validation.

SNET believes a wireless carrier has the right and responsibility to institute a validation process which will insure the integrity of its billing and anti-fraud activities. Towards this end, a unique unit identification is essential.

In order to deliver wireless services successfully and accurately, a carrier must be assured that the identity transmitted from the access device is valid. Without such assurance, the wireless carrier is unable to certify that the device to which the service is delivered is actually that which it proclaims to be. The result is a breach in the integrity of the provider's billing and an invitation to fraud.

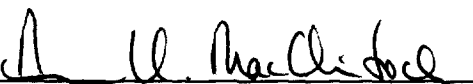
As discussed above, to combat fraud in the cellular wireless arena, legislative action must assure that: 1) the production, modification, possession or use of an unauthorized or modified piece of access equipment, and 2) the production, modification, possession or use of a computer, software, device, piece of equipment or tool which can produce or modify an unauthorized piece of wireless access equipment constitute criminal activities. It is also necessary to allow the sharing of information between parties and with law enforcement agencies to assist in the apprehension and prosecution of the perpetrators. And, finally, to close the door in the long term, the development of unique, tamper-proof mobile unit identifiers is necessary.

IX. Conclusion

In the final analysis, toll fraud affects the entire telecommunications industry. The entire industry has a responsibility to work together to stop fraudulent activity. The Commission has a key role in bringing these parties together.

Respectfully submitted,

The Southern New England
Telecommunications Corporation

By: 
Anne U. MacClintock
Vice President-Regulatory
Affairs & Public Policy
227 Church Street
New Haven, Connecticut 06510
(203) 771-8865

January 14, 1994